Pielikums Nr.1
Iesniegumam par iepirkuma veikšanu

DARBA UZDEVUMS

Būvniecības informācijas sistēmas un papildinājumu drošības testēšana

MĒRĶIS:
Būvniecības informācijas sistēmas (turpmāk – BIS) drošības pārbaude pamatojoties uz Ministru kabineta 2015.gada 28.jūlija noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" (turpmāk – Noteikumi Nr.442) 8., 34.punktu, 2016.gada 27.aprīļa Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (turpmāk - Regula) un papildinājumu drošības pārvaldības novērtēšana atbilstoši Latvijas standartam Nr. LVS ISO/IEC 27001:2009 „Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības" un Latvijas standartam Nr. LVS ISO/IEC 27002:2008 „Informācijas tehnoloģija. Drošības metodika. Prakses kodekss informācijas drošības pārvaldībai", kā arī normatīvo aktu prasībām.

TEHNISKAIS APRAKSTS:
2.1.BIS apraksts:
2.1.1. BIS ir klasificēta kā paaugstinātas drošības sistēma saskaņā ar Noteikumu Nr.442 7.punktu, kuras drošībai pēc minēto noteikumu 34.punkta reizi divos gados ir veicams drošības audits, lai:

- nodrošinātu informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);
- nodrošinātu informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);
- nodrošinātu informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);
- aizsargātu BIS resursus (datnes, arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju, un BIS dokumentāciju);
- aizsargātu BIS tehniskos resursus (datorus, programmatūru, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību);
- noteiktu BIS drošības apdraudējumu (ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana BIS informācijas resursiem var būt traucēta vai neiespējama);
- novērtētu BIS drošības risku;
- atklātu BIS drošības incidentu;
- atjaunotu BIS darbību pēc sistēmas drošības incidenta.

2.1.2. Būvniecības valsts kontroles birojs (turpmāk – Birojs) īsteno darbības programmas „Izaugsme un nodarbinātība" 2.2.1.specifiskā atbalsta mērķa „Nodrošināt publisko datu atkalizmantošanas pieaugumu un efektīvu publiskās pārvaldes un privātā sektora mijiedarbību" 2.2.1.1. pasākums „Centralizētu publiskās pārvaldes IKT platformu izveide, publiskās pārvaldes procesu optimizēšana un attīstība" projektu "Būvniecības procesu un IS 2.kārta" (Nr.2.2.1.1/19/I/005) (turpmāk – Projekts). Projekta īstenošana paredzēta līdz 2022.gada novembrim. Programmatūru izstrādā SIA "Tieto Latvia", atbilstoši 2019.gada 6.decembrī starp Biroju un SIA „Tieto Latvia" noslēgtajam līgumam Nr.5-3.6/2019/50.

Birojs, lai nodrošinātu kvalitatīvu projekta ieviešanu, ir nepieciešama BIS drošības testēšana, kurā pēc katra posma nodošanas atbilstoši Projekta laika grafikam tiktu pārbaudīta BIS jaunizstrādātas funkcionalitātes atbilstība drošības prasībām,.

2.2. Pretendents veic sekojošus darbus:
2.2.1. BIS drošības testēšana, t.sk. ielaušanās testu veikšana:
2.2.1.1. BIS drošības testēšana jāveic saskaņā ar Open Source Security Testing Methodology Manual (OSSTMM) v3.0 standartu un Open Web Application Security Project (OWASP) standartu. Veicot ielaušanās testus, jābrīdina iestāde par iespējamām drošības problēmām, neietekmējot informācijas sistēmas darbības nepārtrauktību. Ir jāveic visu BIS ievadlauku pārbaude attiecībā uz nekorektiem un bīstamiem datiem, kā arī jāidentificē potenciālās drošības problēmas biznesa loģikā un tās jāpārbauda.
2.2.1.2. BIS drošības testēšanas ietvaros Pretendenta galvenie veicamie uzdevumi ir:

- apzināt lietotāju vadības un autentifikācijas ievainojamību (t.i., vājas paroles, nepietiekama autentifikācija, nedrošs paroļu atjaunošanas process, nedroša paroļu uzglabāšana);
- novērtēt riskus, kas saitīti ar sesiju vadību un autorizācijas ievainojamībām (sesijas paredzamība, nepietiekama piekļuves tiesību pārbaude, nepietiekama sesiju likvidēšana, sesijas fiksācija);
- novērtēt riskus, kas saistīti ar lietotājiem „mērķētiem" uzbrukumiem (starp-vietņu skriptēšana, nekonsekventa datu kodēšana, komandu izpilde, operētājsistēmas komandēšana, Structured Query Language (SQL) injekcija, Server-Side Includes (SSI) injekcija);
- novērtēt riskus, kas saistīti ar datu integritātes un konfidencialitātes ievainojamībām (neautorizētas piekļuves iespējamība citu organizāciju/lietotāju informācijai, datu integritātes ietekmēšana);
- novērtēt riskus, kas saistīti ar iespējamu informācijas atklāšanu/noplūšanu (katalogu pārlūkošana, pieejas ceļu modificēšana, paredzamas resursu atrašanās vietas);
- apzināt iespējamos loģiskos uzbrukumus (funkcionalitātes ļaunprātīga izmantošana; pakalpojuma atteice, ievainojamas programmatūras izmantošana, nepietiekama pret-automatizācija, nepietiekama procesu validācija, nepietiekama kļūdu kontrole);
- norādīt citus riskus, ko Pretendents identificē un uzskata par būtiskiem sistēmas pilnvērtīgā testēšanā;
- testēšanai ir jāizmanto manuālās metodes un drīkst izmantot arī automatizētas metodes, standarta automatizētos testēšanas rīkus vai paša pretendenta izstrādātus/modificētus testēšanas rīkus.

2.2.2. BIS drošības testēšanu ir jāveic visām BIS daļām, kuras tiks skartas, izstrādājot jaunu funkcionalitāti Projekta ietvaros. Projekta ietvaros ir paredzēts:

- Pilnveidot būvniecības ieceru un būvprojektu izskatīšanas un saskaņošanas procesu,
- Pilnveidot būvniecības uzraudzības procesu;
- Pilnveidot būvju ekspluatācijas uzraudzības procesu;
- Pilnveidot būvkomersantu datu pārvaldības procesu;
- Pilnveidot būvspeciālistu datu pārvaldības procesu;
- Pilnveidot ēku energoefektivitātes pārvaldības procesu;
- Izveidot būvniecības atkritumu/būvgružu uzskaites procesu;
- Pilnveidot apziņošanas un informēšanas procesu;
- Attīstīt statistiku un kvalitātes mērījumus BIS, t.sk. pilnveidot atskaišu un informācijas analītikas moduļus;

Jaunizstrādāto funkcionalitāti ir plānots nodot pa posmiem. Kopumā Projekta ietvaros būs nepieciešamas 4 BIS papildinājumu drošības pārbaudes: 2020.gada beigās pēc Projekta 2.laidiena

beigām – 1* (viena); 2021.gadā – 1** (viena), 2022.gada – 2 (divas): 2020.gada sākumā – 1** (viena) un 2022.gada beigās pēc programmatūras izstrādes darbu pabeigšanas – 1* (viena) .
* - Ņemot vērā jaunizstrādātas funkcionalitātes ietekmi uz BIS pārbaudes ietvaros jāveic drošības testēšana pilnā apjomā visam BIS.
** - Ņemot vērā jaunizstrādātas funkcionalitātes ietekmi uz BIS pārbaudes ietvaros jāveic drošības testēšana ierobežotā apjomā konkrētiem BIS procesiem.

2.2.3. BIS drošības testēšana jāveic divās kārtās:
2.2.3.1. sākotnējā pārbaude;
2.2.3.2. novērsto apdraudējumu un/vai nepilnību pārbaude.
2.2.4. Par katru drošības pārbaudes kārtu Pretendents iesniedz ziņojumu.
2.2.5. Pretendentam jāiesniedz 2 ziņojumi par BIS drošības testēšanu atbilstoši 2.2.3. punktam. Viens ziņojums par BIS sākotnējo pārbaudi un otrs ziņojums par novērsto apdraudējumu un/vai nepilnību pārbaudi, abi ziņojumi satur 2.2.5.1. līdz 2.2.5.4. apakšpunktos noteiktās prasības.
2.2.5.1. Sagatavotājā ziņojumā jāiekļauj vismaz:

- drošības izvērtēšanā un pārbaudē identificēto ievainojamību un/vai risku apraksts;
- ievainojamību un/vai risku klasifikācija pēc to bīstamības (saskaņā ar Biroja iekšējo risku vērtējumu);
- ieteikumi identificēto ievainojamību un/vai risku mazināšanai.

2.2.5.2. Pretendentam ziņojumam jāpievieno darba dokumenti, kas ļautu izdarīt secinājumus par veiktās pārbaudes darba kvalitāti (veikto pārbaužu apjoms, izmantotie testēšanas piemēri, izmantotie rīki, pārbaudītās ievainojamības un to pārbaužu metodes, u.c.).
2.2.5.3. Piedāvājumā norādītie speciālisti paraksta ziņojumu.
2.2.5.4. Pretendents nodod Pasūtītājam visus ziņojumus latviešu valodā papīra formātā un elektroniski, nosūtot uz e-pastu: pasts@bvkb.gov.lv. Elektroniskajā formātā jāiesniedz dokumentus, kurus iespējams rediģēt un vajadzības gadījumā papildināt ar Pasūtītājam pieejamajiem programmatūras resursiem (Microsoft Office un Microsoft Visio). Citus elektroniskos dokumentus (piemēram, skenētie materiāli) var iesniegt *.PDF, *.TIFF, *.JPG formātos, par to iepriekš vienojoties ar Pasūtītāju.
2.2.6. Pretendentam ir tiesības iepazīties ar BIS papildinājumu izstrādes (Līgums Nr. Nr.5-3.6/2019/50) tehnisko specifikāciju un SIA „Tieto Latvia" tehnisko piedāvājumu un izstrādes laika grafiku Biroja telpās darba dienās no plkst. 9:00 līdz 16:00, iepriekš piesakoties pie vienas no šajā iepirkumā norādītajām kontaktpersonām. Pretendentam būs jāparaksta apliecinājums par konfidencialitātes ievērošanu un informācijas neizpaušanu par SIA „Tieto Latvia" tehnisko piedāvājumu.
Pretendents apņemas neizpaust jebkādu informāciju, ar kuru būs iepazinies Līguma izpildes laikā.

GALAREZULTĀTS:
(aizpilda pakalpojumu iepirkumu gadījumā)
3.1. Veikta kvalitatīva BIS drošības testēšana atbilstoši Noteikumu Nr.442 5.punktam, Regulas prasībām. Sagatavoti 2 ziņojumi (2x2) par BIS drošības pārbaudi un iesniegta MK noteikumu 442 8.punktā minētā aktualizētā drošības dokumentācija.
3.2. Veikta kvalitatīva BIS papildinājumu drošības testēšana atbilstoši Latvijas standartam Nr. LVS ISO/IEC 27001:2009 „Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības" un Latvijas standartam Nr. LVS ISO/IEC 27002:2008 „Informācijas tehnoloģija. Drošības metodika. Prakses kodekss informācijas drošības pārvaldībai", kā arī normatīvo aktu prasībām, kā rezultātā sagatavoti ziņojumi par BIS drošības pārbaudi – 2 ziņojumi (2x2) pēc konkrētas programmatūras izstrādes darbu nodošanas.

PAREDZAMAIS DARBA VEIKŠANAS LAIKS UN VIETA:
4.1. Datu centra un serveru telpu fiziskās drošības un vides drošības novērtējums jāveic Valsts ieņēmumu dienesta telpās - Talejas ielā 1, Rīgā, LV – 1026 un/vai Zaķusalas krastmalā 1, Rīgā, LV - 1050.

4.2. Ziņojumu nodošanas vieta – Būvniecības valsts kontroles birojs, K. Valdemāra iela 157, Rīga, LV – 1013.
4.3. Darba veikšana jānodrošina ievērojot šādu laika grafiku:

- sākotnējā drošības pārbaude jāveic 20 darba dienu laikā no Pasūtītāja rakstiska pieteikuma saņemšanas; novērsto apdraudējumu un/vai nepilnību pārbaude, ja sākotnējā pārbaudē ir konstatēti apdraudējumi un/vai nepilnības, jāveic 10 darba dienu laikā pēc Pasūtītāja rakstiska pieteikuma saņemšanas;
- ziņojums par katru no pārbaudes kārtām jāiesniedz pirmās un otrās kārtas pārbaudes termiņu ietvaros;

4.4. Iepirkuma līguma darbības termiņš ir līdz 2022.gada 31.decembrim.

Pasūtītāja pārstāvis I.Zapoļskihs